DRAFT

Dr. Paul Twomey
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers
(ICANN)

Keynote Address
Media Connect Influence Forum
Hunter Valley, Australia

Sunday, 9 September 2007
12:00 noon – 1:00 p.m.

Ladies and gentlemen and colleagues, welcome and thank you for your interest in attending this forum. I'd especially like to thank Phil Sim and the team at Media Connect for extending the invitation to present today's keynote speech.

In the brief time I have today, I'd like to focus on a few key aspects of the future of the Internet from my perspective and highlight some important challenges facing Australia if it is to successfully play a role in that future Internet.

Brief Introduction to ICANN

Before we begin, I'd like to give you some background about ICANN's origins, its mission and its four closely linked goals.

ICANN was created in 1998 as an international multi-stakeholder organization responsible for the technical management and coordination of the Internet's domain name system and its unique identifiers. It is responsible for coordinating the Internet's —

- Internet Protocol address space allocation;
- Protocol identifier assignment;
- Generic and country code top-level domain name system management; and
- Root server system management functions.

In fulfilling its mission, ICANN is guided by four founding principles:

- To preserve the operational stability and security of the Internet, particularly the domain name system;
- To promote competition and choice for registrants, especially in the generic top-level domain arena;
- To achieve broad representation of global Internet communities;
- And, to develop policy appropriate to its mission through bottom-up, consensus-based processes.

These are the concepts ICANN stands for —

- Ensuring a single, interoperable Internet
- Providing a means for all to express their own language and identity
- Providing access by all others
- Encouraging creativity, development, growth and innovation, particularly at the edge of the network

- Maintaining security of the network to ensure confidence in the model

- Ensuring stability of the experience for application development and consumer experience

- Deploying resources efficiently in support of a global network

- Ensuring all relevant stakeholders have a voice and role

So, while ICANN is keenly interested in all the developments surrounding the Internet, its user community, and their demands for increased functionality, there is much that ICANN cannot directly manage or even influence. Our most important role continues to be a consensus-builder of policies and protocols affecting the security, stability, and interoperability of the global Internet well into the future.

The rapidly evolving Internet and what its future holds

In less than 40 years, we have seen the Internet burgeon from a single purpose — to transmit files and simple electronic messages — to a complex network of networks, the infrastructure we've come to depend on not only for communicating, but also for transacting business, transferring and storing data, and gathering together in virtual communities around the world.

In looking forward another 10 years one can never have certainty. Indeed the comments in my next part of my speech are personal, not those of ICANN. This search into the looking glass is merely that of one individual.

While it's difficult to be definitive about the future, here are some things I think we can expect:

- Usage of the Internet will be limited only by access to electricity. As many as 3 billion people may be able to enjoy a truly global Internet.

- Many, perhaps most, will access the Internet by using mobile devices.

- We’ll see a very significant increase in broadband access (over 100 mb/sec indeed up to 1 gigabit per second). Many developing countries such as Morocco, China, and Malaysia are adopting accelerated broadband distribution programs to deliver the Internet to their citizens.

- A machine-to-machine Internet will overtake today’s person-to-person Internet.

- We will see billions of Internet-enabled appliances at home, at work, in the car, and in the pocket.

- Third parties will use the Internet to monitor all sorts of activities and utilities — from washing machines to cars to electricity meters.

- Geo-location and geo-indexed systems will be much more common and emergency services will be more precisely dispatched.

- There will be significant improvement in spoken interaction with Internet-based systems.

- We will see an even wider array of delivery methods for intellectual property (movies, sound tracks, books, and so on) than is available today. VoIP will be prevalent and SIP may be the principal protocol means by which calls are set up. Voice communication will be essentially free, except perhaps for calls that terminate on traditional PSTN devices including mobiles.

- Almost no industry will be offline since most will rely on the Internet for customer interaction, customer discovery, sales, service, advertising, and similar activities.
- Group interaction and collaborative support tools — including distributed games — will be very common.
- And last but certainly not least, internationalized domain names and new gTLDs will open up the Internet to much more multilingual content.

What will you be able to do in the future that you can't do now? Here are a few examples:

- Manage your appliances and home security systems through online systems.
- Use your mobile phones as remote controllers.
- Download videos, music, and books as an everyday practice. Video on demand will focus on watching previously downloaded video rather than watching streaming, real-time video. This is really just an obvious extrapolation of the iPod/TiVo paradigm.
- You will be able to talk to the Internet itself to search for information and interact with various devices — and it will respond.

- Search systems will be more precise because meta-tagging of information will have become more common. This is part of the semantic web movement.

- Maintenance histories of products that can be serviced will be keyed to radio frequency IDs or bar codes associated with the devices. This is one potential use of Internet Protocol version 6, or IPv6, which is the natural extension of the original IPv4.

What will the technical underpinnings of the Internet look like by then?

- Terabit per second local networking will be available as backbones for local networks.

- The domain name system will operate in multiple language scripts. Again, a result of deploying IDNs and new gTLDs.

- IPv6 will be widely deployed, once the technical and financial issues have been worked out.

- Better confidentiality and authenticity will be provided through the use of a public key crypto. This will provide more authentication all along the network.

- Much more inter-device interaction will be common, incorporating position location, sensor networks, and local radio communications.

- Spam, phishing, and various forms of denial of service attacks will continue a cold war-style arms race with defenses and better authentication techniques.

- Operating systems will continue to be troublesome sources of vulnerability.

What will everyone — businesses, other organizations, and individual users alike — still need to worry about?

- Spam and phishing
- Attacks on the domain name system
- Attacks at routing
- Fraud/IP spoofing
- Cyber protests

I will speak more about this shortly.

So what are the consequences of such a vision for Australia?

First and foremost, for Australia to gain the significant economic, social, and government services advantages of such a future Internet, broadband — proper broadband — will need to achieve near universal distribution. Second, Australia will need a comprehensive approach to build national resiliency in the face of cyber-crime and cyber attack threats. Third, Australian governments, ISPs, and enterprises must recognize that Internet Protocol version 6 is the technology of today and that they must transition from the IPv4 technology of yesterday.

Broadband will be absolutely essential and so will re-engineering the economy

There should be no confusion: the broadband speeds required to participate in the Internet in 10 years' time will be measured in the 100s of megabits per second. Indeed, network planners in South Korea are now moving households to 1-gigabit connections today.

Why is the appropriate approach to broadband so important? Because the Internet will continue to represent a massive and accelerating force for the reduction of transaction costs across the global economy, and a force for unprecedented innovation in the delivery of private and public services. Since European settlement, Australians have built a modern trading economy based on the swift uptake of information and communication technologies. Now is not the time to fail to appreciate the ongoing revolution of those technologies.

The public debate in Australia on broadband needs to shift now from how to why. The key question to ask is, Broadband for what? The answer is a revolution in the delivery of private and public sector services to Australians and to our customers overseas. The rapid growth in video-based applications, including now high definition videoconferencing, will be at the heart of delivering a more human-centric online interaction for Australians of all ages and skills.

Today in Britain, the healthcare of aged people is monitored and managed through multi-party videoconferencing tools, with the result of greater efficiency in healthcare delivery and improved outcomes for aged citizens, many of whom stay in their own homes much longer than previously available. Imagine the impact on GDP if the delivery of all sorts of services to Australian citizens in a human-centric way is available in the house. Imagine the impact on rural communities — imagine the national savings impact of managing an ageing population in their homes for much longer than now is the average — imagine the impact on service enterprises through the re-engineering of their delivery services to capture greater efficiencies and improve customer experience! This is what the public debate about broadband should now focus on. Just as floating the dollar drove a re-engineering of the Australian economy, so a broadband network for all Australians should drive a re-engineering of our economic and social delivery systems.

Broadband is not merely about network — it is about micro-economic reform.

But we will need to plan for it — not just for the network but for the unique opportunity it will give corporate, social, and government entities to re-engineer their processes. When all the world is available to a customer or citizen through his or her screen, there is no point in continuing to try to serve them with approaches suited to the 1970s.

Building national resilience to withstand a worsening security environment will be essential

Beginning on 28 April 2007 and lasting for weeks, the small Baltic nation of Estonia became the target of a very large cyber attack. The attacks were mostly targeted against specific Estonian market infrastructure — banking, news, and so on — and against local, county, and national government sites. There has been a great deal of speculation as to the reason for this attack, which focuses on existing tensions between ethnic and expatriate Russians and Estonians.

This event more than any other has brought to light the idea of a new battlefield. Those with an army of zombie computers — that is, a botnet — whether government-sanctioned or owned by a private entity, can cause significant damage to an individual, corporation, core Internet infrastructure, or even an entire country. Those with enough knowledge and resources can launch a very large-scale attack that could possibly have enormous impact on a global scale.

Botnets are run by organized crime and leased to any party, for any purpose. A botnet can be used for economic purposes — spam or phishing — or it can be used for political and terrorist purposes. These attacks could be against infrastructure, whether it be critical Internet infrastructure, the core infrastructure of a large corporation, or the physical infrastructure or plant that relies on the Internet that is not adequately protected against DDoS and other types of Internet-based attacks.

If we look at the Estonia attack, we see that an attack against a country can be conducted with a frightening fluidity. Estonia is one of the better connected countries in the Baltic region, and the April attack was debilitating. There are many countries in less-developed regions that would simply drop off-line in an attack of that scale.

Botnets are becoming more sophisticated as the tools to find and fight them are developed. The traditional botnet is a collection of zombies with a single command-and-control point, using protocols such as IRC channels to monitor and send attack instructions. Recent analyses suggest that botnet “herders” are evolving to peer-to-peer models with distributed command-and-control centers and diverse instruction channels.

On 17 January 2007 a new Internet trojan infestation was detected. This “Storm Worm” — so dubbed by Finnish company F-Secure — attacked computers using the Microsoft Windows operating system. The trojan spread very rapidly, beginning in Europe and quickly moving to the United States. As of Monday, January 22nd, just five days after detection, the trojan accounted for 8% of all infections world-wide.

It appears that the goal of Storm Worm was to acquire a very large botnet.

Current estimates as to the size of the “Storm Bot” range dramatically, anywhere from 250,000 to over 5 million infected computers. Though the Storm Bot has delivered billions of spam emails a day, most of that spam is payload mail intended to propagate the botnet. Canadians are also attributing the Storm Bot to the wide-spread DDoS attack against Canadian websites during the weekend of August 11th. It is speculated that the attacks — if they were indeed from the Storm Bot — were not aimed at any particular websites and were probably a test of its DDoS capabilities.

Though there have been some incidents that can be attributed to the Storm Bot, it is believed that the botnet is merely in its growth and test phase. New mechanisms to deliver the trojan payload have been seen evolving, such as emails stating that your face is on YouTube, and similar devices.

Once fully active, this botnet will be of epic proportions. A botnet that combines more than 5 million computers to be used in a direct attack scenario will be utterly and completely crippling to the targeted computers.

Using botnets for DDoS attacks can range from retribution against a person or a company, or for extortion and political and/or terrorist activity. Taking the attack on Estonia as an example; it appears that the lead-up to the attack began as a cyber riot during which Russian chatrooms were filled with individuals agitating others about the events in Estonia. They would then supply very simple commands for regular users to type to contribute to the cyber riot. Some of the people offered the service of their botnets pro bono, and the cyber riot was then enhanced by botnet attacks. While similar attacks have taken place between Israeli and Palestinian netizens, at the time of the Kosovo-Serbian struggle, and between Chinese and U.S. netizens during the April 2001 Hainan Island incident, this is the first widely publicized case of cyber protesting.

Though botnet DDoS attacks are spectacular, the real money lies with the other malware that sits on a bot, or infected machine. Many of these bots contain multiple programs intended to do many things. Bot herders sell the bots to distribute spam emails by the millions. Most alarming, though, is the keystroke loggers that come with many of the malware packages. These loggers collect data the user puts into the computer, most specifically credit card information and bank login credentials. The bot then sends this information on to the botnet herder and the herder in turn puts them on auction or uses them to siphon cash. The real money lies with the phishing data, and the botnet as an attack vector, though frightening, is still a secondary business product.

Most of the Big Bots these days are programmed by professionals. There are still the script kiddies and available scripts that can exploit or take over websites, but the real culprits are the cyber criminals. They make a lot of money and can pay for very professional software. There is a non-existent entity known as the Russian Business Network (RBN) that is notorious for housing malware, phishing, and cybercrime sites. This is becoming big business.

Would Australia be able to survive an attack similar to the one launched on Estonia with less disruption? Perhaps, considering Australia is a much larger country with a more widely dispersed infrastructure base. However, the country still has some way to go in terms of national preparedness — especially in the face of increasingly widespread, sophisticated attacks.

While coordination of key federal agencies has improved significantly and planning is under way, there is a need to recognize that, unlike some other emergency scenarios, cyber attacks require a very broad-based response.

The vast majority of Internet resources are in the hands of the private sector — and not just the hands of the critical infrastructure providers. They are distributed throughout the nation's financial services, media, retail, energy, wholesale, trading, and other sectors. As Estonia showed, it is the websites that attract millions of users, as well as the network providers, which are the greatest points of vulnerability.

This reality poses a completely new challenge to Australian security planning. Government is not the only key to online security — it is coordination with a widely defined private sector that will protect Australian citizens and their economy from interruption. And this is not a question of talking to the Chief Information Officers of technology companies. It is essential to educate and engage the CEOs of Australia's most consumer-popular companies. It is their decisions about suppliers, websites, and customer interactions which are at the heart of improved security. And the same is true for state and municipal government agencies. The CEOs of Australia's major banks have shown the leadership to ensure close cooperation with key agencies in the face of cyber-attack risk. Others need to follow suit.

Moreover, in an online world, the key is to work to build business and economy-wide resilience, not to pretend that one can build a water-tight defense. The upkeep of defenses AND the practice of what to do when they are breached is key.

One priority for the emerging coalition of government agencies and industry sectors is to practice domestic scenarios. War-gaming is essential if people are to be prepared. And such exercises must include the business and political leadership. Knowing when and how and what to message to a community under cyber attack is just as important as it would be in the case of a pandemic influenza outbreak. Political and business leaders are prepared and rehearsed for what to do if there is an avian flu outbreak. They are not so prepared for a massive cyber attack or protest. And they need to be.

When the 7 July 2005 bombings took place in London, the world was impressed by the response by London — it was a testament to the careful consideration of the risk and regular practice of response.

If Australia were to suffer a serious national cyber attack, it is doubtful if such an appraisal could be made.

The federal and state governments, together with industry associations like the Business Council of Australia, must work closely to understand the challenge of just what vulnerabilities have accompanied the great benefits of building a networked economy, and then to work on jointly alleviating these risks.

This work must not just be allocated to technicians and officials. It is important to involve leaders.

What the Estonia attacks show is that as societies become more reliant on Internet technologies, these technologies become a conduit for protest and attack by the disaffected.

Australia must become IPv6 ready

As you know, each of the billions of devices connected to the Internet must have a unique numerical, or IP, address. But the spectre of a bank barren of IPv4 addresses has loomed over the Internet community for many years. In fact, as of June of this year, only 19 percent of IPv4 addresses remains. The 128-bit IPv6 technology solution — and there are potentially 340 trillion trillion trillion of them — extends the current 32-bit IPv4 protocol, enabling continuing and future expansion.

Aside from allowing continued Internet expansion, IPv6 will —

- Allow every machine or device to have its own IP address, simplifying network design and facilitating remote configuration.
- Allow for very high bandwidth networks by making use of larger data packets, a benefit to academic, educational, and scientific institutions.
- Open the door to next-generation devices we haven't even thought of yet — but will.
- Enable better connectivity worldwide, allowing remote operation of home and office appliances and devices.
- Increase the possibility of real-time data retrieval and transmission across the Internet.
- And a potential commercial advantage: gaining understanding of new technology sooner rather than later.

Is the move to IPv6 inevitable? The short answer is, Yes. But, IPv4 will not disappear any time soon, even in the face of the increasing urgency to adopt IPv6. Individual ISPs may not easily handle the increased network load. The increase in routing level loads is also of concern.

- There is no cutoff date for IPv4 address block allocations yet.
- Both systems will run in parallel for the foreseeable future.
- And the possible reintroduction of unused IP addresses into the system is being explored as well.

The IPv6 allocation and transition policies have been drawn up. We are now focusing on resolving the technical and financial issues that have arisen in the Internet community.

So, where are we now?

- The pool of unallocated IPv4 addresses is projected to be fully distributed within 3 to 5 years.
- The perception of IPv6 deployment as merely a technical issue — and some disagreement within the technical community — have slowed the move to IPv6
- However, many organizations and governments are now stressing its importance publicly.

There are at least five groups that can and should move actively toward adopting IPv6:

- Federal and state governments need to revisit the work they prepared two years ago to set a policy to encourage IPv6 adoption, especially inside government itself.

- Internet Service Providers need to offer IPv6 transport service. This will be a growing business opportunity. ISPs need to require vendors to supply IPv6 capable routers, management systems, and so on.

- Content providers should also recognize the opportunity to offer content via IPv6 as early as possible.

- Very importantly, CIOs of enterprises need to plan their network's transition to IPv6 now. They should list all the enterprise's dependencies on IPv4 and extinguish them incrementally. This job needs planning and time. Action should be now, not when the unallocated IPv4 pool exhausts.

- Finally, vendors need to continue developing fully capable IPv6 devices. They should ensure that these devices operate at the same performance standards as IPv4.

Conclusions — Observations —

The Internet is the most powerful and pervasive means of empowering individuals in recent human history. It is becoming part of the glue that ensures a rapid unleashing and sharing of humanity's knowledge and possibilities for all persons no matter their age, sex, class, ethnicity and — at least in some degree — wealth. And it is radically breaking down the obstacles to a global community.

It requires the continuing efforts of all stakeholders, from governments, the business and private sectors, academia, and civil society to preserve and strengthen this model. By doing so, we can ensure the resiliency and utility of the Internet — and guarantee the rapid and successful development of a secure, stable, and globally interoperable Internet.

Finally, allow me once again to express my personal delight at being invited to this Media Connect Influence Forum.

Thank you. I will now take questions.